Model-based Risk Analysis of Security Critical Systems

Siv Hilde Houmb[1], Trond Stølen Gustavsen[1], Ketil Stølen[2], Bjørn Axel Gran[3]

[1] Telenor R&D, Norway, {siv-hilde.houmb, trond-stolen.gustavsen}@telenor.com

[2] Sintef Telecom & Informatics, Norway, kst@sintef.no

[3] Institute for Energy Technology, bjornag@hrp.no

CORAS (www.nr.no/coras) is a EU funded R&D project (IST-2000-25031) developing a methodology and a framework for model-based risk assessment based on AS/NZS 4360 [1]. CORAS focus on security critical systems in general, with particular emphasis on IT security. IT security includes all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of IT systems (ISO/IEC TR 13335-1:2001 [2]). The focus is on controlling risks by using well know risk analysis methods from the safety domain, such as HazOp [3], FMEA [4] and FTA [5], which have been used within for example the chemical and nuclear industry since World War II [3].

The presentation will focus on how to use UML (Unified Modeling Language) behavioural diagrams [6] as input diagrams to risk analysis. The approach will be exemplified by demonstrating how a UML sequence diagram can be used to support HazOp for risk identification. Our approach includes both guidelines on how to construct the input diagrams from existing system documentation and how to perform a risk analysis using a particular input diagram.

The presentation will conclude with summarising some of the preliminary results from the CORAS project, with emphasis on how we have and will verify the usability of the methodology developed within the project and in particular the methodology developed for using input diagrams to support risk analysis.

References

1. AS/NZS 4360:1999 Risk management (1999).
2. ISO/IEC TR 13335-1:2001: Information technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security.
3. Leveson, Nancy G., "SAFEWARE, System, Safety and Computers", Addison-Wesley, ISBN: 0-201-11972-2, 1995.
4. Bouti, A., Ait Kadi, D., A state-of-the-art review of FMEA/FMECA. International Journal of Reliability, Quality and Safety Engineering 1 (1994), 515-543.
5. IEC 1025:1990 Fault tree analysis (FTA) (1990).
6. Booch, Grady, Jacobson, Ivar, and Rumbaugh, James, "The Unified Modeling Language Reference Manual", Addison-Wesley Longman Inc., ISBN: 0-201-30998-X, 1999.